State of Arizona
Government Information Technology Agency

Technology Infrastructure Standards Assessment (TISA)

Background
An annual IT Security Assessment is required to be submitted to GITA by each Group 1 agency per statewide IT Planning Policy, P136, and Risk Management Standard, P800-S805. In addition, Arizona's implementation plans for domains within the Enterprise Architecture call for gaps from target technology usage to be addressed as part of each agency's annual IT planning activities. An online self assessment tool, Technology Infrastructure Standards Assessment (TISA), addressing IT quality assurance and enterprise architecture as well as IT security compliance is available at www.azgita.gov/apps/.

Purpose
The purpose of the self-assessment is threefold: 1) assess current overall standards compliance among Group 1 agencies; 2) educate these agencies as to current security and enterprise architecture standards; and 3) aid them in identification of their IT security vulnerabilities as well as deviations in complying with other statewide standards. Any vulnerabilities and compliance deviations should then be addressed in the agency's IT plan.

Requirements
Each major executive branch agency must assess its IT environment, using the TISA application, by September 1st of every year. Mid-year updates to TISA are encouraged, if there has been significant change to an agency's risk posture (either an increase or decrease), by justification of each proposed change on agency letterhead in advance and submittal to GITA Homeland Security manager.

For FY 2007, 25 categories are being assessed: 17 of the categories deal with IT security, two are in the area of software architecture, one in the area of network architecture, one in the area of platform architecture, three in the area of data/information architecture and one in the area of quality assurance. These categories correspond with the statewide standards found on the GITA web site at www.azgita.gov/policies_standards/. The questions are extracted from each referenced standard with the specific paragraph number indicated in parentheses at the end of each question. Only a handful of questions have changed from the FY2006 TISA.

Agencies are requested to estimate their approximate percentage of compliance for the current and next three fiscal years in each of these categories. The intent is to use weighted and aggregated data to identify potential statewide trends across multiple agencies. For FY 2007, a threshold of 70% compliance has been set for responses to all standards including security, although the intent is to drive this threshold upward in future years. It is expected that agencies will comply with not only the letter of the standards, but the spirit of them as well. Indeed some agencies will surpass the standards by applying 'best-in-class' solutions. Security, especially back-up, standards compliance should always strive toward a 100% compliance level.

Note changes from previous years: Use of "Not applicable" is strongly discouraged and needs to be negotiated with GITA in writing in advance. In addition, zero percent compliance will also

require a written justification to GITA as statewide standards were adopted to apply to all agencies. Again, resolution of gaps or compliance not reaching 100% within the next three years should be addressed in the agency's IT plan as either an IT goal or objective including annual targeted performance measures. The year of 100% compliance to each standard is no longer requested. High-level logical network diagrams can now be uploaded as DOCUMENT from within TISA.

Questions?

For access into the TISA application or general questions, contact the IT Planning Manager at 364-4784. For specific questions regarding a standard, contact either the Enterprise Architecture Manager (jryan@azgita.gov) at 364-4790 or for specific questions regarding IT security; contact the Homeland Security Technology Manager at 364-4771.